Fraud Crimes, Trends & Typologies

Strategic Analysis Report

Financial Intelligence Unit, P. O. Box 854, King Abdullah Bin Abdulaziz Al Saud ST, Abu Dhabi, UAE.
Phone no: 97126919955
Email address: uaefiu@uaefiu.gov.ae

TABLE OF CONTENTS:

List of Acronyms

FFIU	Foreign Financial Intelligence Unit
FFR	Fund Freeze Report
FI	Financial Institution
FPP	Federal Public Prosecution
FRR	Fund Recall Request
goAML	The Financial Intelligence Unit online reporting application
HRC	High Risk Country Transaction Report
HRCA	High Risk Country Activity Report
LE	Legal Entity
LEA	Law Enforcement Authority
ML/TF	Money Laundering and Terrorist Financing
MOI	Ministry of Interior
PNMR	Partial Name Match Report
PP	Public Prosecution
RE	Reporting Entity
RFI	Request for Information
RFR	Reason for Reporting
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
STR	Suspicious Transaction Report
UAE FIU	Financial Intelligence Unit of the UAE
UNODC	United Nations Office on Drugs and Crime

Objective

This Project is part of the Strategic Analysis Plan (SAP) adopted by the UAE FIU also considering the requirements of the *National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates* (NRA) and the following *UAE National Action Plan to Implement the Combating Anti-Money Laundering and Terrorism Financing National Strategy 2020-2023* (NAP).

This Report presents the results of the strategic analysis relating to Fraud trends and typologies along with associated risks identified during the analysis.

The purpose of this Report is to:

- Enhance the knowledge of Fraud types and its characteristics.
- Understand the nature of the environment in which Fraud occurs.
- Identify trends, typologies and repeated Fraud types.
- Promote a level of awareness and knowledge of the phenomenon to the public and private sectors.

Methodology

The strategic analysis has been carried out based on the Strategic Analysis Methodology adopted by the UAE FIU, ensuring a structured and comprehensive risk-based approach, in view of developing raw data and information into knowledge and intelligence to be used in policy and decision-making processes, and operational activities.

The analysis and conclusions illustrated in this Report are based on the analysis of data and information held by the UAE FIU, as well as other data and information obtained from domestic and international stakeholders /sources, particularly in the period 2019-2021.[1]

[1] The data and information analyzed include but are not limited to: STRs and SARs databases; information received from UAE Authorities; information received from counterpart FIUs and Reporting Entities.

وحدة المعلومات المالية
Financial Intelligence Unit

Introduction

In general, **Financial crimes** refer to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else, to obtain a financial or professional gain.

Financial crime is also known to be relatively consistent with offences like, but not limited to, fraud and cyber-crime, money laundering, and terrorist financing.

Fraud crimes is a serious threat globally. While escalating at an alarming rate, the estimated losses due to it is also accelerating. Accordingly, regulators and institutions in the financial sector (and other relevant sectors) should understand the threats and vulnerabilities surrounding such crimes and implement measures to protect themselves and their customers.

By its nature, the scale of financial crimes is difficult to trace or figured. For example, the United Nations Office on Drugs and Crime (UNODC) highlighted that "the clandestine nature of money-laundering" makes it difficult to accurately estimate the total amount of money being laundered every year globally. The most common estimate for the amount of money laundered globally in one year is 2 to 5% of global GDP, or 800 billion – 2 trillion USD.[2]

According to publicly available information, it is reported that the total losses of financial crime globally has crossed three (3) trillion US dollars.[3] According to estimates[4], e-commerce losses pertaining to 'online payment fraud' is estimated to be at USD20 billion globally in 2021. Whereas, in the United Kingdom (UK), it was estimated that GBP 92 million has been lost through dating scams in the year of 2021 alone.

In the UAE, Fraud is also a focus topic being one of the most common crimes facing the financial sector. Fraud crimes are committed every single day – a risk that all governments worldwide are facing and attempting to combat. While law enforcements and other bodies are tracing and prosecuting financial criminals, fraudsters develop more sophisticated methods to commit such crimes.

The estimated losses related to international 'fund transfer fraud' (based on information collected from the reporting entities as well as the received suspicious reports by the UAE

[2] https://www.unodc.org/
[3] https://www.clari5.com/
[4] https://www.statista.com/

FIU) is approximately AED 152 million in 2020 and AED 132 million in 2021. Whereas the estimated losses related to the domestic 'fund transfer fraud' is approximately AED 154 million in 2020 and AED 162 million 2021.[5]

Background

Fraud is a criminal offense that refers to the intentional deception to secure or gain unfair or unlawful profit or to deprive the legal right of a property ownership. Fraud involves a misrepresentation of facts either by words or by conduct, withholding of vital information, or even making false statements made by one party (perpetrator) to another, causing Financial or non-financial or potential loss to another party (victim).

In the law context, fraud is a felonious act; countries have legal frameworks that ordinarily impose criminal and civil penalties for it. There are elements to define fraudulent acts. For an incident to be called 'Fraud', there are some basic elements to be present, such as (but not limited to):

- Purposeful deception (i.e. a false statement, a misrepresentation of facts)
- The intention (the perpetrator intent to deprive the victim of something usually money/exchangeable assets)
- Prejudice (the victim suffering potential or actual loss because of the fraudulent activity).

Apart from the above listed elements, other circumstances would also lead to the occurrence of fraud incidents. An old hypothesis that was developed by a known criminologist called the 'fraud triangle' highlights three factors aiming to understand why fraud is committed. The said factors were: first is 'opportunity', second is 'motivation' or 'pressure', and last is 'rationalization'.

In the context of Financial Institutions, fraudsters usually exploit the weaknesses and gaps in three factors: first, being the personnel of the institution; second, is the internal Policies and Procedures; and third is the systems infrastructure.

[5] Estimates based on information collected from the reporting entities as well as the analysis conducted on the received suspicious reports by the UAE FIU.

As previously mentioned, an individual or group of individuals can perpetrate fraud, or even larger groups known as Fraud Organized Crimes or Fraud Syndicates. As there are countless types of fraud evolving worldwide every day, this report will present the main Fraud trends and techniques identified by the UAE FIU, and will exemplify sanitized cases illustrating the identified schemes.

The analysis presented in this report are based on a broad range of data and information, including, but not limited to, the databases owned or directly accessible by the UAE FIU particularly the Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) database. The data and information requests received from UAE Authorities, such as the Federal Public Prosecution and Local Police Departments, and counterpart Financial Intelligence Units (FIUs), particularly in the period 2019-2021.

Additional information have been requested from selected Reporting Entities (REs), which provided the UAE FIU with useful inputs contributing to the ongoing analysis and identifying relevant trends and typologies as well as some relevant risk factors.

Overview of the relevant data and information underlying the strategic analysis

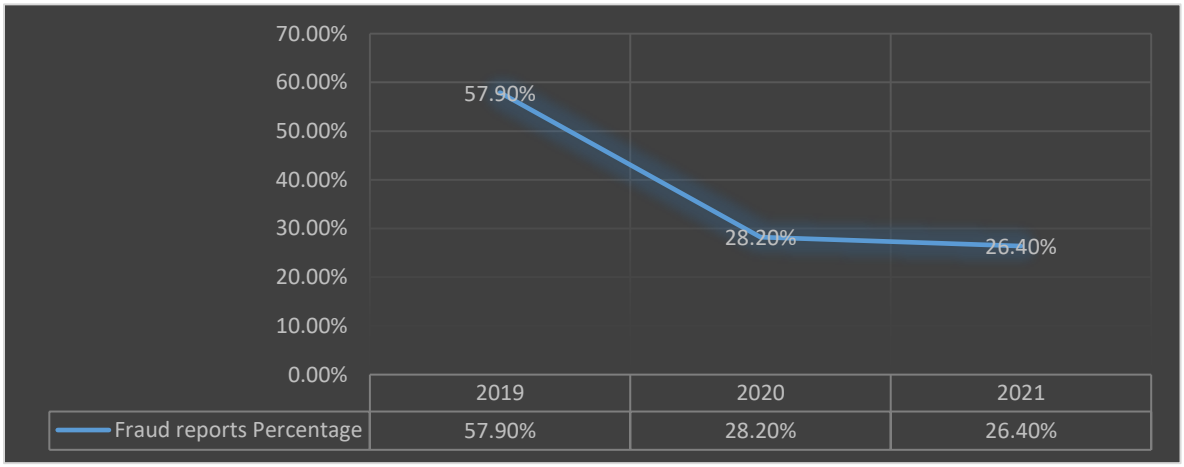
1. Review of Suspicious Reports received by the UAE FIU

During the period from 2019 until 2021, UAE FIU received a total of 49,469 suspicious reports, those reports include **Suspicious Transaction Reports (STRs)** and **Suspicious Activity Reports (SARs)**. A noticeable increase in the figures was observed in the overall received STRs and SARs during the said period, however, decrease observed in those related to 'Fraud'. This can be attributed to:

- the efforts of the Supervisory Authorities, Law Enforcement Authorities (LEAs) and UAE FIU in increasing the 'Fraud' awareness in financial sector of the UAE;
- actions taken against the subjects committing the Fraud by the Law Enforcement Authorities; and
- UAE FIU's efforts in taking prompt action in stopping further disbursement of fraudulent funds.

The table below presents the percentage of Fraud related reports received by the UAE FIU compared with the overall suspicious reports.

Year	Legacy STR reporting system	goAML	Total Fraud-Related STRs/SARs	Overall STRs/SARs Received	Fraud reports Percentage
2019	6,167	1,300	7,467	12,880	57.9%
2020	-	4,659	4,659	16,522	28.2%
2021	-	5,294	5,294	20,067	26.4%



NOTE: The above table does not include other report types included in the goAML (i.e. High Risk Country Transaction Report "HRC", High Risk Country Activity Report "HRCA", Partial Name Match Report "PNMR" and Fund Freeze Report "FFR"), only STRs and SARs were considered.

When looking at the "Reason for Reporting" selected by the reporting entities pertaining to the Fraud related STRs/SARs, in order to identify the underlying Fraud types, it was noted that for 2021; the majority of reports received (39%) were concerning 'Scams', followed by (26%) concerning 'Domestic funds recall requests', and a very close estimation of 14% and 13%, related to 'Online baking fraud/account take-over' and 'International funds recall request', respectively.

Reason for Reporting "RFR"	Percentage from overall Fraud Reports (based on RFR)		
	2019	2020	2021
Customer is transferring funds on behalf of unrelated third parties for a commission – possible fund transfer scam	2%	2%	2%
FRAUD – Advance fee fraud/Phishing or email fraud/Inheritance fraud/fake prizes frauds/romance fraud	48%	51%	39%
FRAUD – Apparent resubmission of rejected loan application with key borrower details changed from individual borrower to company; this activity may identify the same person attempting to secure a loan fraudulently through a non-existent person.	0%	0%	0%
FRAUD – ATM/Card Skimming frauds	1%	0%	0%
FRAUD – Charity/donations fraud activity	1%	3%	0%
FRAUD – Cheques deposited from a possible funnel account appear to be pre-signed, bearing different handwriting in the signature and payee fields – forged cheques	2%	0%	0%
FRAUD – Corporate Fraud	0%	1%	1%
FRAUD – Customer provides forged record of past or present employment on a loan application.	2%	1%	2%
FRAUD – Customer tries to conceal/forge identification documents or declines to produce originals for verification.	3%	2%	2%
FRAUD – Employee frequently overrides internal controls or established approval authority or circumvents policy. (Staff Fraud)	1%	0%	0%
FRAUD – False/fraudulent insurance claims	0%	0%	0%
FRAUD – Falsification of certified cheques, cashiers cheques or non-cash item cheques drawn against a borrower/buyers account, rather than from the account of a financial institution.	1%	0%	0%
FRAUD – Fund Recall Request – Domestic	8%	26%	26%
FRAUD – Fund Recall Request – International	6%	13%	13%
FRAUD – Low appraisal values, non-arms length relationships between short sale buyers and sellers, or previous fraudulent sale attempts in short-sale transactions.	0%	0%	0%

1. Review of Inward Spontaneous Dissemination (ISD) and Inward Request of Information (IRI) from foreign Financial Intelligence Units

In the same review period, the UAE FIU received **314 intelligence reports** from foreign Financial Intelligence Units (FFIUs) concerning suspicions related to "Possible Fraudulent Activities". On the other hand, UAE FIU sent **122 intelligence reports** to counterpart FIUs related to the same concerns. The reports categorized into the below principles:

Main Suspicion	No. of Requests from Counterpart FIUs			
	2019	2020	2021	Total
Possible Fraud	70	62	47	179
Possible Business Email Compromise Fraud	1	8	19	28
Possible Forgery	4	12	9	25
Possible fraudulent wire transfer	1	5	18	24
Possible Investment Fraud	1	12	11	24
Possible fraudulent documents	0	5	4	9
Possible Breach of Trust - Fraud	0	1	6	7
Possible Ponzi schemes	0	2	3	5
Possible Pyramid Schemes	0	0	3	3
Possible VAT/Excise Frauds	0	1	2	3
Possible Counterfeiting and piracy of products	1	0	1	2
Possible Counterfeiting currency	0	0	2	2
Possible ATM Fraud - Cash trapping Crime	0	1	0	1
Possible Identity Fraud or Identity Theft	0	0	1	1
Possible internet fraud - Hacking	0	0	1	1
Total	78	109	127	314

For the purpose of this study, the UAE FIU conducted analysis on a sample of approximately 20% of all the incoming international intelligence reports (inward requests for information and inward spontaneous disseminations). The outcome of the

International Cooperation "IC" requests' review coincides with the results of STRs/SARs review.

Similarity of trends and techniques found from the international requests received and the STRs/SARs reported by local reporting entities, which will be further discussed in the latter part of this report. It was additionally noticed that majority of aforementioned intelligences were received from certain counterpart FIUs in strategically relevant countries.

2. Fund Recall Requests received by the Financial Institutions in the UAE

A request for information regarding international repatriation requests received related to fraud was sent to 235 reporting entities composed of domestic banks, foreign banks/representative offices and money exchange houses. Out of the total, 178 REs (76%) responded to the UAE FIU's request with only 22 reporting entities (9%) confirming that they have received such requests from international counterparts.

Collectively, the responding 22 reporting entities received 698 repatriation requests with a total amount of approximately AED 179M in 2020, and 726 repatriation requests amounting to around AED 169M in 2021.

The table below illustrates summary of the international fund recall requests received by FIs in 2020 and 2021 from several jurisdcitions along with successful recalls related to the fraud-related requests. *(All amounts are in AED).*

INTERNATIONAL FUND RECALL REQUESTS (2020-2021)					
2020			2021		
No. of Fund Recall Requests Received	Total Amount Involved (in AED)	Total Amount Successfully Recalled (in AED)	No. of Fund Recall Requests Received	Total Amount Involved (in AED)	Total Amount Successfully Recalled (in AED)
698	178,892,183	26,552,149	726	168,976,357	36,554,195

In 2020, approximately AED 27 million (15%) out of the total international fund recall requests was successfully recalled to the requesting banks from their respective

jurisdictions, on the other hand, successful fund recall requests increased to almost AED 37 million (22%) in 2021.

A similar request for information pertaining to domestic fund recall requests related to fraudulent transactions was sent to the top reporting entities of Fraud related STRs/SARs, out of which 20 reporting entities confirmed receipt of fund recall requests related to local fraudulent transfers.

Below figures are the number of domestic fund recall requests received and total amount involved during 2020 and 2021 along with successful recalls related to the fraud-related requests.

DOMESTIC FUND RECALL REQUESTS (2020-2021)					
2020			2021		
No. of Fund Recall Requests Received	Total Amount Involved (in AED)	Total Amount Successfully Recalled (in AED)	No. of Fund Recall Requests Received	Total Amount Involved (in AED)	Total Amount Successfully Recalled (in AED)
2,458	170,255,327	16,022,834	2,164	168,733,844	5,958,496

In 2020, the successful fund recall requests amounts to AED 16 million (9.41%) out of the total fund recall requests received by banks and exchange houses in the UAE from other financial institutions, while in 2021, the percentage has decreased to around AED 6 million (3.53%). The reason of decrease could be two folds; one is the delay in interventions from the remitting bank (victim's account), second could be the rapid usage and dissipation of funds by the perpetrator(s) leaving the account with no balance or minimal balance for the repatriation to be successful. The expenditure of funds might be through Cash withdrawals (mainly) or funds subsequently transferred being to other bank account(s), domestically or internationally.

3. Domestic Cooperation Requests

The exchange of information with other UAE Authorities is another element we looked at during the review of this study. Over the period of **July 2019** until **6 June 2022**, the UAE FIU received **10,707 requests** from local stakeholders such as **Ministry of Interior (MOI)**, **Federal Public Prosecution (FPP)**, and different **Police Departments**. Approximately

3.24% of the said requests were concerning Fraud and/or Cyber-crime queries and/or investigations.

Trends and Typologies

All data and information gathered and presented in this report, have been subject of in-depth analysis by the UAE FIU to identify related trends and typologies. The UAE FIU has reviewed approximately 1,000 STRs/SARs and around 62 ISDs/IRIs, by the end of the review, the UAE FIU observed some repeated trends and fraud types / activities as described below:

- 'Funds Transfer Fraud' or Money Transfer Fraud"

One of the most common fraud types that have been observed in the received suspicious reports, it is also perhaps considered as one of the most financially damaging as it involves significant amount of funds. Fund Transfer Fraud is a wire/electronically transferred funds that are of fraudulent nature. Such incidents (in most scenarios), are followed by 'funds recall request' or so called as 'repatriation request', sent by the remitting bank (victim's account) to the beneficiary bank (perpetrator or fraud accomplice's account).

The fraudulent funds received in the perpetrator's account are usually dissipated rapidly either by cash/cheque withdrawals or subsequently transferred to another account(s) as in more complex cases. From the review of data the funds received suspected to be either a proceeds of fraud crime that occurred outside the UAE (International fund transfer fraud), or a proceeds of fraud crime occurred inside the UAE (Domestic fund transfer fraud).

By its nature, the level of compromise that open the doors to criminals for fraudulent transactions cannot be tightened to one aspect. It commonly involves 'cyber-attacks' via malicious hacks (malware or virus) enabling the fraudster to attain victim's credentials and vital information to conduct fraudulent transfers, or rather be associated with internal or external frauds some of which are further explained below.

- Business E-mail Compromise (BEC)

During the analysis of data for this report, it was observed that Business E-mail Compromise is one of the main concerns of which counterpart FIUs has mostly queried.

The term refers to a type of cyber-attack (usually by hacking or phishing), and would involve impersonating a company's official to conduct unauthorized transactions. This scheme generally starts either with exploitation of publicly available information, or hacking of an individual or organization's email (spoofing). After obtaining sufficient information that could be used for the commission of BEC fraud, perpetrators typically use other prevalent techniques to deceive the victims.

For instance, the fraudster would pretend to be a supplier or service provider and would trick the buyer/user of the service into changing bank account payee details. This is also called as Redirection Fraud.

Another example is when the perpetrator posing as a legitimate supplier, sends e-mail to its target asking for payment against the alleged or genuine goods/services to be provided to the target. The sender's email address is usually an imitation of the legitimate supplier's email address – only that spelling could be changed, acronym could be used or another domain that looks similar to the supplier's actual domain could be utilized, etc. The fraudulent email is commonly accompanied with forged supporting documents, such as contract agreement, invoice, bill of lading, etc. Included in the invoice is the "supplier's" bank details, wherein perpetrator intentionally modifies the bank account number only (in fact owned by the perpetrator or an accomplice) so that transfers will be directly received by the fraudster or the accomplice.

- Scam Fraud

A scam is another deceptive scheme observed during our analysis. Over the years, scammers constantly evolve and develop sophisticated techniques to deceive their targets (victims) into divulging their confidential information and/or credentials in order to gain monetary or personal benefits.

From the review of STRs/SARs, the following are the common techniques/modus operandi used by fraudsters to trick its victims:

- Fake Products/Fake Websites Fraud: Commonly, perpetrators act as: (1) seller of products in popular social media websites and advertising their products in lower price than its actual market value. Usually consumers prefer the savings benefit they may obtain from purchasing these products at a lower cost. Products may truly exist, however, the brand and its features are essentially substandard. On the other hand,

the suppliers may have received the payment online but products will never be delivered to customers, as there is no existing products in reality; (2) customs employee informing the customers that there is an incoming shipment for them. The perpetrators tend to ask for variety of customs fees in order for the shipment to be successfully delivered to them. In many instances, more than one individual collude to deceive the expecting victim.

- Fake Visa/Ticketing Fraud: Perpetrators act as a legal travel agent offering visa or ticketing service and asking for the payment to be completed online before proceeding to the issuance of visa or ticket. However, after the transfer has been made, the travel agent poser stops communicating with its victim.

- Investment Scam/Fraud: This type of fraud has been widely known ever since, regardless of the current economic situation and time. Investment fraud is noted to have caused major financial losses, not only to individuals but also to many companies. Its main characteristic is that the perpetrator tends to offer an investment (more often fictitious) to its target that promises high return with little or no risk. The prospective investments in this type of scam are usually in three forms: company shares, real estate, and stocks.

  Moreover, due to the current development in financial banking and increasing demand of virtual currencies, criminals have also found ways to exploit its features for fraudulent activities including investment scams.

  Furthermore, from the review of the intelligence reports received from counterpart FIUs, it highlighted that UAE's financial system has been possibly targeted or used in disguising the proceeds of fraudulent activities occurred abroad.

  - Phishing / Vishing

Refers to a fraud type, where fraudsters obtain victim's sensitive information or credentials either online (phishing) or by phone calls (Vishing). In phishing attacks, the victim would usually need to click on a malicious link and would ask the victims to enter their information on the background. This click might download a malware or viruses to the device used by the victim enabling the attacker to obtain all entered information. In most common scenarios, the attacker will create a fake or what looks like a website of a financial institution and would give the victim some steps to follow. While in vishing, the fraudsters

use different ways and social engineering techniques to convince victims into revealing their personal or sensitive information willingly over the phone.

- Forgery / Counterfeit

Forgery is unlawfully altering an instrument or a document with the intention to deceive another party. For example 'Signature forgery', which involves illegally replicating someone else's signature. Another example is 'cheque forgery', which involves making unlawful alterations to the details such as the amount, or it might be paired with signature forgery.

On the other hand, counterfeit is unlawfully making an imitation of a genuine instrument or document. For example, creating totally false identity documents, making fake cheques, or counterfeit currencies, and generating false invoices.

Risk Indicators

Due to the large variety of fraud types, sources, and categories and that each type preserve its own characteristics and red flags, the UAE FIU have established some generic risk indicators that might be directly or indirectly relevant to Fraud.

The presence of such indicator in a situation can raise suspicions and trigger investigation leading to further identification of other indicators. Nevertheless, a criminal activity cannot be explicitly concluded based on a single indicator, but a simultaneous occurrence of it along with the analysis of other available information may suggest that Fraud crime is committed.

Herein some developed 'Red Flag' indicators that could possibly alert the risk of Fraud:

- A customer submitting documents suspected to contain any materially false, fictitious, or fraudulent statement or entry.
- A customer knowingly falsifies, conceals, or covers up via any trick or scheme a material fact or makes any materially false statement or representation.
- Discrepancies observed between reported facts, observed data, and/or supporting documentation.
- Inadequate or apparently altered supporting documentation (such as, alterations to any vital information, scraps, spelling mistakes, etc.).

- Supporting documents that contains vendor receipts and/or other supporting documents that appear to be altered (obvious white-out areas, cuttings, deletions).

- 'Funds recall requests' received from different remitting banks on the same beneficiary.

- Funds received via wire transfers (international or local) from unrelated parties, followed by immediate withdrawals or outward remittances.

- Incoming funds transfer followed by 'Funds recall request' from the remitting bank.

- Frequent incoming funds transfers from unrelated parties to a newly opened account(s).

- Insufficient justifications obtained from the account holder on the received funds, or a customer that clearly unaware of the purpose and source of funds received in the account.

- Accounts opened for 'Salary' purpose especially individuals as low-income workers with no actual salary income witnessed in the account, instead the account receiving multiple remittances or deposits from unrelated parties.

Other 'Red flag' indicators (Financial / Behavioral):

- Unusual transactions or inter-account transfers (including relevantly small amounts).

- Rising costs with no explanation or that are not commensurate with an increase in revenue.

- Employees who appear to make a greater than normal number of mistakes, especially where these lead to financial loss through cash or account transactions.

- Employees who are subject to complaints and/or tend to break the rules and who also request details about proposed internal audit scopes or inspections.

وحدة المعلومات المالية
Financial Intelligence Unit

Case Examples

Case Example (1): Advance Payment Fraud

The UAE FIU received two (2) STRs concerning two individuals (Person A and Person B) who have defrauded a victim (XY) through "Advance Payment Fraud" and "Social Media Fraud". Person A initially contacted Person XY through a social media application informing him that a parcel containing branded perfumes, iPhone and luxury watches intended for him will be delivered after shipment charges is paid.

On the next day, Person B, acting as a customs officer, contacted Person XY regarding the same parcel and demanded additional payment for customs clearance fees. Subsequently, Person B contacted Person XY again asking for insurance and other miscellaneous fees to be paid.

Person XY abided to all the three payment requests and sent the funds through an exchange house. After receiving all the transfers, Person A and Person B stopped communicating with Person XY on his queries and no parcel nor a refund was received.

UAE FIU has conducted its in-depth analysis on Person A and Person B. Apparently; the subjects are involved into fraudulent activities, mainly Advance Fee Fraud, victimizing individuals from some repeated nationalities.

UAE FIU disseminated the case to LEA for further investigation. As per LEA's feedback, the subjects were seem to be involved into fraudulent activities and a money laundering case was opened.

Red Flags identified:

- Receipt of funds from different unrelated individuals

- Beneficiary of funds belongs to low-income workers category.

- Account turnover not in line with KYC profile

- Extensive use of social media to communicate with the customers

Case Example (2): Vishing

UAE FIU has received multiple SARs from a single reporting entity related to a common modus operandi being used by fraudsters to defraud their customers.

The victims, mainly citizens and residents, approach the reporting entity complaining about a new beneficiary added to their mobile/internet banking but denying creation of it.

Initially, the victim receives a vishing call from the fraudster and through social engineering techniques, the fraudster is able to convince the victim to divulge his/her personal information, including the name, EID number and bank details.

UAE FIU approached the reporting entity to enquire about the repeated pattern observed in the SARs filed by them. The reporting entity responded and stated that their customers involved in the SARs are victims of vishing scam, whereby the banking information including OTP was shared with the fraudster who then create an internet banking profile by using the victims' details and then added a new beneficiary for fraudulent purposes. The reporting entity further added that they have conducted a review and confirmed that the beneficiary process on their electronic channels is supported by OTP verification, which implies that the beneficiary cannot be added to the customer's beneficiary list without the OTP being sent by the reporting entity to the registered mobile number of the customer. The new beneficiary is either added by the fraudster or the customer itself after receiving the OTP.

Although there were number of reports related to the same modus operandi, the reporting entity confirmed no recorded financial loss.

Case Example (3): Application Fraud/Forgery

UAE FIU has received multiple STRs from several reporting entities, including domestic banks and finance companies, regarding fraudulent activities conducted through falsification of documents or forgery.

Typically, a fraudster approaches the reporting entity with the purpose of applying for a credit facility (personal/car loan, credit cards). The reporting entity asks for supporting documents to assess eligibility of the applicant. The documents include, but not limited to, passport, national ID, residence visa (for residents), proof of income, labor contract, etc.

The documents presented mainly contain falsified salary certificate (inflated), labor contract, visa, and statement of accounts (forged) to the reporting entity during application of a credit facility.

During the UAE FIU's investigation of the STRs related to the same fraud method, the following are some of the common findings established:

- The supporting documents coming from the company (i.e. salary certificate, labor contract) have the actual company's stamp and required signature from the authorized personnel (applicable for individuals only).
- After being granted with the credit facility, the perpetrators tend to leave the country after paying no or few instalments.
- The credit-takers use previous job's salary certificates and other company details to apply for a new credit facility.
- The perpetrator, posing as a legitimate employee of a certain company, provides supporting documents which are entirely forged. For instance, fake company details, forged visa details and labor contract, and inflated salary in order to pass a bank's eligibility criteria.

The UAE FIU has disseminated similar fraud type to the Law Enforcement Authorities in the UAE, in which feedback received stated that cases were added to their databases.

Conclusion

In conclusion, the impact of fraud goes beyond just financial losses, Fraud impact individuals, institutions in different sectors, industries, and economies. For Financial Institutions, the reputational losses would be more damaging than the financial losses suffered from Fraud. For that reason, Financial Institutions must understand how fraud crimes are committed and find the most effective measures to detect and prevent such incidents to safeguard their customer's and their own interests.

Fraud risk assessments, including root-cause analysis, would assist institutions to define and implement a proper management plans and measures. Additionally, the fraud risk assessment will also focus on identifying and addressing vulnerabilities and the risk environment surrounding both internal fraud (i.e. embezzlement and misappropriation of assets) and external fraud (i.e. hacking and theft of assets or information) and therefore establish preventative and nevertheless detective controls (both manual and automated).

Unfortunately, Fraud crimes is not an issue that will simply disappear. Global and national efforts needed to tackle it strategically, adding to it the benefit of being proactive rather

than reactive. Awareness, prevention, detection controls as well as internal investigations are all necessary elements to be integrated in an effective anti-fraud strategy, and its success will be of great benefit.